UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	Case No. 6:22-mc-892
Xbox One X gaming console, s/n 111921174117, currently located at FBI, 211 E. 7th Ave, Ste 320, Eugene, Oregon 97401, as described in Attachment A	

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Xbox One X gaming console, s/n 111921174117, currently located at FBI, 211 E. 7th Ave, Ste 320, Eugene, Oregon 97401, as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2) and (a)(5) and (b)(1)	Receipt and Possession of Child Pornography

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Deane Rawlinson Davis, FBI, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 2:05pm a.m./p.m. *(specify reliable electronic means)*.

Date: September 13, 2022

Judge's signature

City and state: Eugene, Oregon

Mustafa T. Kasubhai, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF DEANE RAWLINSON DAVIS

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Deane Rawlinson Davis, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since 2021. I am currently assigned to the Eugene Resident Agency (EURA). In this position I am tasked with investigating federal crimes within EURA's area of responsibility, to include child exploitation and possession, distribution, and production of child pornography. Prior to my employment with the FBI, I was a sworn law enforcement officer employed by the Washington State Liquor and Cannabis Board (WSLCB) from 2017-2021. I have completed training at the FBI Academy at Quantico, Virginia, and the Washington State Criminal Justice Training Commission – Basic Law Enforcement Academy. For most of my employment with WSLCB I was assigned to the Marijuana Enforcement Unit, where I was tasked with investigating criminal and administrative violations with a nexus to marijuana in Washington State. I have received additional training in Criminal Investigations, Interdiction Operations, Cell Phone, Social Media and Digital Investigations, and am a certified NIK Polytesting Drug Identification Instructor/Trainer. In my official law enforcement duties, I have written and participated in the execution of search warrants, both for physical locations and electronic data. I am a currently a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of an Xbox One X gaming console, s/n 111921174117 (hereinafter the Device) which is currently

stored, in law enforcement possession, on the premises of the FBI Eugene Resident Agency Evidence Control Room, 211 E. 7th Ave, Ste 320, Eugene, Oregon 97401, assigned FBI item no. 1B1 in FBI case number 305D-PD-3638049. As set forth below, I submit that probable cause exists to believe and do believe that the items set forth in Attachment B constitute evidence of contraband, fruits, and instrumentalities of violations of Title 18, United States Code, §2252A, involving the receipt, and possession of child pornography.

3. This affidavit is intended to show only that sufficient probable cause exists for the requested warrant and does not set forth all of my knowledge regarding this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Relevant Statute

4. As set forth below, I submit that probable cause exists to believe, and do believe, that the Device contains evidence of the following violations:

> **Title 18 U.S.C. § 2252A(a)(2) and (a)(5) and (b)(1) (Receipt and Possession of Child Pornography)** provides in part, that whoever, knowingly receives any child pornography that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempts to do so, shall be fined and imprisoned not less than 5 years and not more than 20 years (for receipt, there is not mandatory minimum sentence for possession).

Statement of Probable Cause

Summary

5. In May of 2022, Richard Garrett was on supervised release, as a result of a conviction for distribution and possession of Child Pornography in the District of Oregon (6:13-cr-00343-MC). Garrett was prohibited from possessing any unapproved internet connected devices. During a home visit by Probation Officer Dallin Hudson, it was discovered that Garrett had been using an unapproved, internet connected, Xbox. An Xbox is a gaming console that can also be used to access the internet and to send and receive emails. Garrett admitted to having hidden the device and admitted to having created an email account to receive Child Pornography (CP). An email consistent with the one provided by Garrett as being used to receive CP was accessed multiple times on the Device. Access to the aforementioned email was followed by numerous MEGA URLs, at least one of which had a sexually explicit filename, thought it could not be confirmed to be child pornography. I believe that Garrett was using the Xbox to access an encrypted email and encrypted cloud storage in order to view and receive CP, and that evidence of these crimes will be located on the Xbox.

Richard Garrett Background

6. On June 21, 2016, Richard Earl Garrett was sentenced to 120 months for Distribution of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) and Possession of Child Pornography in violation of 18 U.S.C. § 2252A(a)(5)(b) and (b)(2). Garrett was released October 1, 2021. Upon release, Garrett was to be supervised for a period of 10 years, until September 30, 2031.

7. Special Conditions of Supervision included, but were not limited to, the

following:

a. The defendant shall submit to a search of his/her computer (including any handheld computing device, and electronic device capable of connecting to any on-line service, or any data storage media) conducted by a U.S. Probation Officer, at a reasonable time and in a reasonable manner, based upon reasonable suspicion of a violation of a condition of supervision. Failure to submit to a search may be grounds for revocation. The defendant shall warn all individuals that have access to defendant's computer that it is subject to search and or seizure.

b. The defendant is prohibited from using or possessing any computer(s) (including any handheld computing device, and electronic device capable of connecting to any on-line service, or any data storage media) without the prior written approval of the U.S. Probation Officer. This includes but is not limited to, computers at public libraries, Internet cafes, or the defendant's place of employment or education.

c. The defendant is prohibited from accessing any on-line computer services at any location (including employment or education) without prior written approval of the U.S. Probation Officer.

Xbox One Located

8. On May 25, 2022, U.S. Probation Officer (USPO) Hudson and USPO Robinson conducted an unannounced home visit at Garrett's residence. During the home visit, USPO Hudson noticed a television in Garrett's room was connected to an Xbox console with a "Call of Duty" type game on the screen. The screen displayed a conversation with another user, leading USPO Hudson to believe that the device was connected to the internet, in violation of Garrett's

special condition.

9. When asked about the device, Garrett admitted that it was connected to the internet and that he was aware that violated his special condition. Garrett also admitted to having a Nintendo Switch, which was not authorized, but said it was not connected to the internet. Garrett stated that he had been using the Xbox since approximately December of 2021. Garrett admitted that he had hidden the Xbox from USPO Hudson on previous home visits.

10. USPO Hudson reviewed the Xbox on site and noted recent use of the Microsoft Edge App. Microsoft Edge is an internet browser that is used to browse the internet from internet connected Xbox Consoles. According to the Microsoft website:

> "Browse the web right from your Xbox console. Just launch the Microsoft Edge app and you can keep up with your favorite sites on the internet, watch videos, and even play games – all without leaving your console. Edge on console also supports playing some games with an Xbox controller, using a mouse, private browsing, cross-platform syncing of Edge from your other devices, and using a passkey."

Upon opening the Edge browser USPO Hudson observed two movies, and pornographic chats. When asked, Garrett confirmed he had viewed pornography on the Xbox. Garrett initially stated everything he viewed was adult pornography.

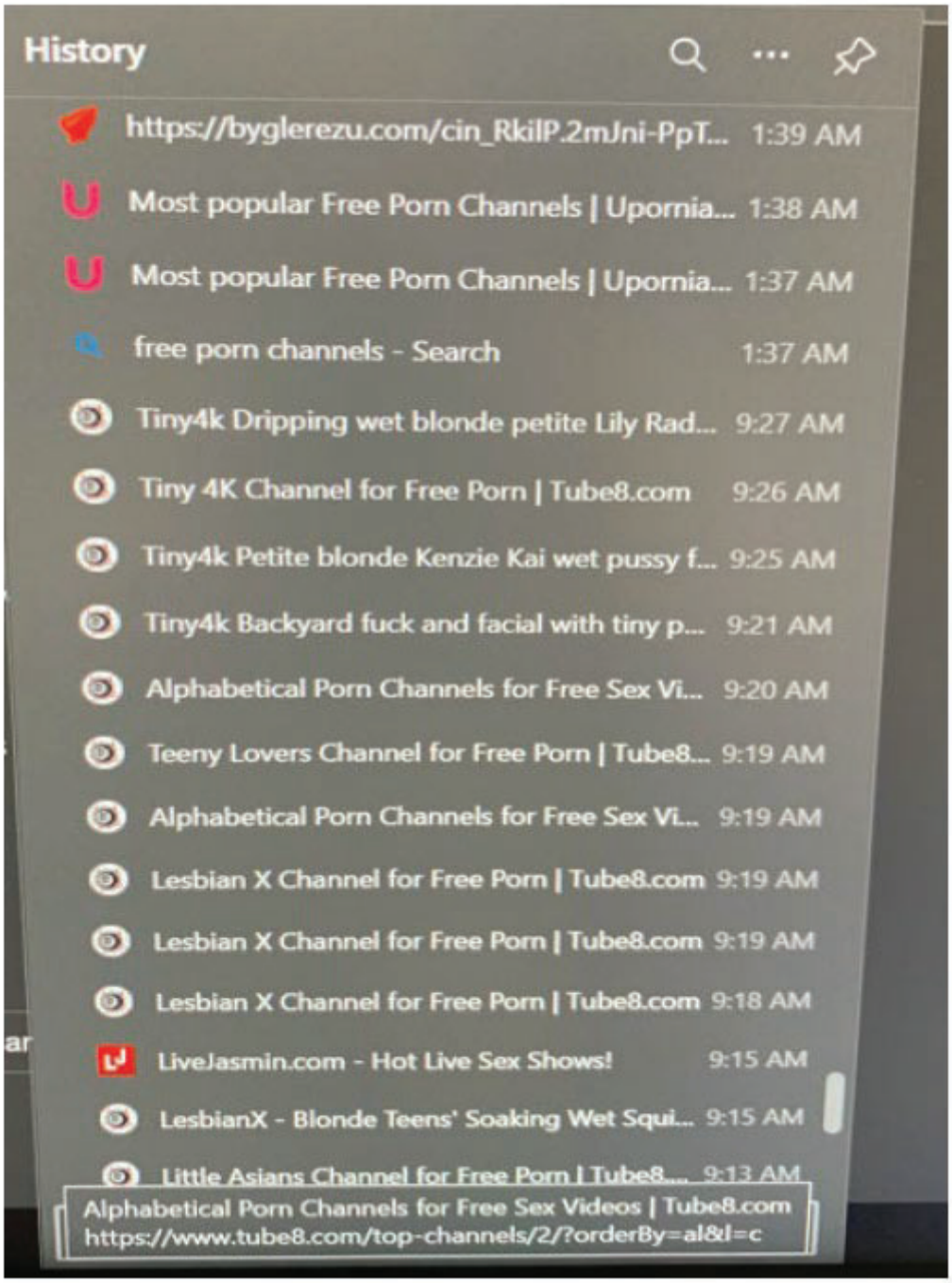
11. USPO Hudson explained that the Xbox would be seized as it was in violation of Garrett's special conditions. USPO explained to Garrett that the Xbox may be forensically examined and asked if anything would be found on the device. Garrett admitted to having watched CP for a period of about one month. Garrett admitted that he created an email account to receive CP from someone else. Garrett stated the email account he created to receive CP was

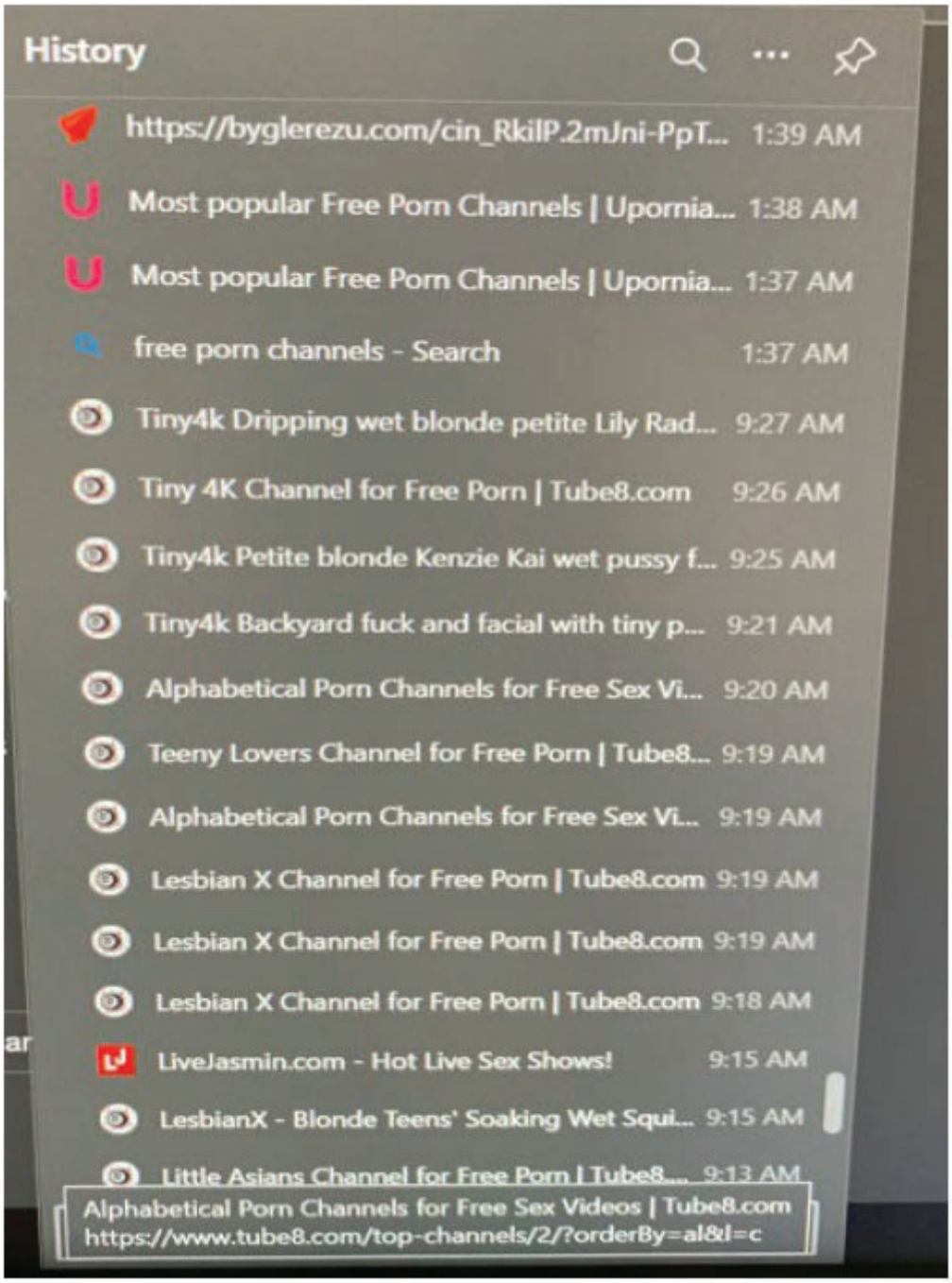
something along the lines of "alenjonessmith", but he didn't remember the rest.

Preliminary Review by USPPS

12. On July 11, 2022 Terry Ginsberg, a Computer Forensic Investigation and Recovery Search Team Examiner (hereinafter examiner) with United States Pretrial and Probation Services (USPPS) conducted a preliminary review of the Xbox seized from Garrett's residence. The examiner removed the console hard drive and created a clone of that drive, which was exported to another hard drive with similar specifications. The clone drive was placed into the console and the system was turned on. The examiner performed a manual review of the device and took screenshots of any relevant activity.

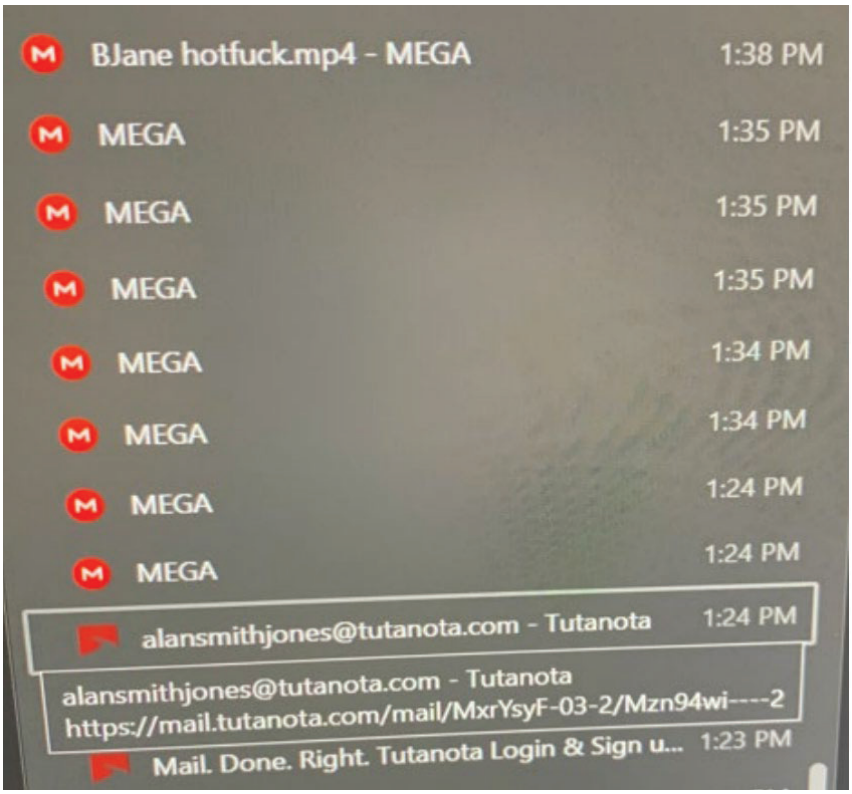
13. The examiner was able to access and review Edge browser history on the device. The browser history revealed the console user regularly visited websites which host pornographic content. This was evidenced by inspection of the webpage titles and some of the URLs. The URLs appear to be commercial sites that have adult pornography. Below are examples of the sites that were visited:

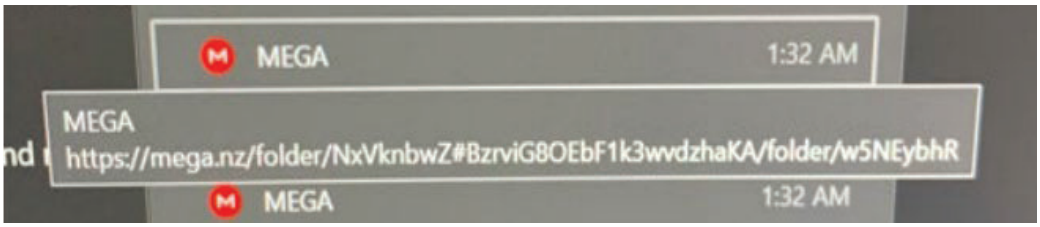

History
https://byglerezu.com/cin_RkilP.2mJni-PpT... 1:39 AM
Most popular Free Porn Channels | Upornia... 1:38 AM
Most popular Free Porn Channels | Upornia... 1:37 AM
free porn channels - Search 1:37 AM
Tiny4k Dripping wet blonde petite Lily Rad... 9:27 AM
Tiny 4K Channel for Free Porn | Tube8.com 9:26 AM
Tiny4k Petite blonde Kenzie Kai wet pussy f... 9:25 AM
Tiny4k Backyard fuck and facial with tiny p... 9:21 AM
Alphabetical Porn Channels for Free Sex Vi... 9:20 AM
Teeny Lovers Channel for Free Porn | Tube8... 9:19 AM
Alphabetical Porn Channels for Free Sex Vi... 9:19 AM
Lesbian X Channel for Free Porn | Tube8.com 9:19 AM
Lesbian X Channel for Free Porn | Tube8.com 9:19 AM
Lesbian X Channel for Free Porn | Tube8.com 9:18 AM
LiveJasmin.com - Hot Live Sex Shows! 9:15 AM
LesbianX - Blonde Teens' Soaking Wet Squi... 9:15 AM
Little Asians Channel for Free Porn | Tube8... 9:13 AM
Alphabetical Porn Channels for Free Sex Videos | Tube8.com
https://www.tube8.com/top-channels/2/?orderBy=al&l=c



While only adult pornography sites appear in this list, that is consistent with his statement that he searched for adult pornography on the internet and obtained child pornography via his email.

14. In addition to the aforementioned activity, the examiner also noted a series of browsing events involving Tutanota email and MEGA cloud storage. On at least three occasions the user accessed an email account alansmithjones@tutanota.com. Each time the user accessed the email, the user would then proceed to access numerous MEGA links. This email is very similar to the email recalled by Garrett as the email created and used to receive CP. The user appears to have repeatedly accessed a possible video file by the name of BJane hotfuck.mp4 while browsing MEGA after accessing the Tutanota email. MP4 is a common file extension for video files. Based on this pattern of browsing activity, it is reasonable to believe that the user was accessing MEGA links received via the Tutanota email which Garrett admitted was created to receive CP.





15. One Megalink URL (above) was visible in the screenshots provided by USPPS. FBI attempted to visit the URL to determine if it contained CP, but the link was no longer valid. I know hosting sites like Mega.nz and Dropbox, often take down or block these links when they are flagged for illegal content, making the content inaccessible. Users can also deactivate links they generate, as described below. For this reason, it is common for collectors to download and save copies of images they receive in the form of hyperlinks, or cloud storage links.

Tutanota Background

16. Tutanota is an email service that allows users to send and receive end-to-end encrypted emails to other Tutanota users, and to third party services by providing a password that acts as an encryption key. Tutanota also allows unencrypted emails to be sent that are stored on Tutanota's encrypted servers. Email contents and attachments are automatically encrypted. Tutanota encryption is done locally on the user's device. Tutanota automatically assigns an asymmetric key pair (one private, one public) on the customer's device, rather than on the Tutanota servers, which eliminates the company's ability to access user's data. Tutanota offers one email address with up to one Gigabyte of storage for free and allows users to pay for up to one Terabyte of storage and up to 100 email aliases. Tutanota also offers an encrypted calendar and address book.

Mega Background

17. Mega Limited is an online secure cloud storage company that is based in New

Zealand. Users that sign up for Mega are offered 50 gigabytes of free online ("Cloud") storage space. Mega also offers paid plans for additional storage. Mega can be accessed by navigating to the website of https://mega.nz/, or by using a mobile device and accessing the Mega.nz application or "app". Mega's services are end-to-end encrypted (i.e. Mega is not able to view their users' content). Some of Mega's services include the ability to access your Mega account via any web browser connected to the Internet, live encrypted backup/file synchronization, and web browser extensions. Mega also offers users mobile applications (apps) that can be downloaded from Apple's App Store, or the Google Play Store.

18. Some of Mega's mobile apps include Mega Chat which is also end-to-end encrypted. Mega Chat allows users to chat with another Mega user or multiple Mega users at once (group chat). Mega Chat users can share files with other Mega users directly from their Mega cloud account. Within Mega chat, users can make encrypted audio and video calls.

19. Mega users can share their files from their Mega Cloud account by generating a unique link to send to other users to click on to share the files they directed to be shared. Once a Mega user generates a unique link to a share a file or files located on their Mega cloud account, that data then becomes unencrypted and anyone with that link can access the files that person to share. Additionally, the Mega user who chooses to generate a unique link to share a file or files can set an expiration date to the link, that is, after a certain amount of time that link becomes inactive, and the content is not available to access. Unique Mega shared links can be copied and pasted and "re shared", in other words a Mega user can not prohibit the re-distribution of shared links.

Digital Device Background

20. The Device is currently is currently stored, in law enforcement possession, on the premises of the FBI Eugene Resident Agency Evidence Control Room, 211 E. 7th Ave, Ste 320, Eugene, Oregon 97401, assigned FBI item no. 1B1 in FBI case number 305D-PD-3638049. The device was seized as described above by USPPS. Based on my conversation with the USPPS examiner, I know that the Device was stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as it was when the Device first came into the possession of the USPPS. On September 1, 2022 the Device was transferred to the custody of the FBI. The device was entered into FBI evidence and then transferred to the FBI Eugene Resident Agency, located at 211 E. 7th Ave, Ste 320, Eugene, Oregon 97401.

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Additionally, data that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. I submit that probable cause exits to believe that data once stored on the device will still be stored there because, based on my knowledge, training, and experience, I know that:

a. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore,

deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, email programs, and chat

programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Lastly, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from

law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

Nature of Examination

23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to

human inspection in order to determine whether it is evidence described by the warrant.

24. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

25. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

26. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

27. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the

data contained therein.

28. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

30. Based on the foregoing, I submit that probable cause exists to believe, and I do believe, that the Device described in Attachment A contains evidence of contraband, fruits, and instrumentalities of violations of the above-described crimes, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Device described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

\ \ \

\ \ \

\ \ \

\ \ \

31. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Amy Potter, who advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

/s/ Deane Davis, Per rule 4.1
Deane Rawlinson Davis
FBI, Special Agent

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 2:05pm a.m/p.m. on September 13, 2022.

HONORABLE MUSTAFA T. KASUBHAI
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is an Xbox One X gaming console, s/n 111921174117 with hard drive (hereinafter the Device) which is currently stored, in law enforcement possession, on the premises of the FBI Eugene Resident Agency Evidence Control Room, 211 E. 7th Ave, Ste 320, Eugene, Oregon 97401, assigned FBI item no. 1B1 in FBI case number 305D-PD-3638049.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of Title 18 U.S.C. § 2252A(a)(2) and (a)(5) and (b)(1) (Receipt and Possession of Child Pornography) and involve Richard Earl Garrett from December 1, 2021 through the date of the execution of the search warrant, including:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, or attempt to do so, of images and audio and video recordings of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, including where such images, audio and video were obtained and how and where they were stored;

b. All originals and copies of images and audio and video recordings of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, and material identifying the minors;

c. Identifying information, images, video, audio, contact information, addresses, telephone numbers, email addresses, social media site accounts and usernames for persons with whom Garrett traded, purchased, received, sent, or otherwise dealt in Child pornography.

d. Evidence of the destruction, or attempt to erase, hide or delete the above-described items.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks,

saved usernames and passwords, documents, identifying information and records for accounts, websites social media programs and applications, and browsing history.

3. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used;

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

c. Records of data storage accounts and use of data storage accounts;

d. Records containing screen names, user names, e-mail addresses and identities assumed for the purposes of communicating on the Internet;

e. Internet and cellular data billing and subscriber records.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable

amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of

reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.